UCRL-ID-147478

An IEEE 802.11 Wireless LAN Security White Paper

Jason S. King

U.S. Department of Energy

Lawrence
Livermore
National
Laboratory

October 22, 2001

DISCLAIMER

This work was performed under the auspices of the U.S. Department of Energy by the University of California, Lawrence Livermore National Laboratory under Contract No. W-7405-Eng-48.

1. Background

Given the increased productivity and growing popularity of wireless communications in general, and wireless data communications in particular, this paper outlines the protocols, security implications, and architectures of IEEE Std. 802.11-1999 wireless LANs (WLANs) and makes recommendations regarding a phased implementation of WLANs at LLNL.

This project is driven by the need for convenient and secure access to the Internet for Laboratory visitors and to the internal network for Laboratory employees. A solid architecture designed with a priority on security will allow LLNL to offer network access in areas where it is traditionally hard to deploy "wired" networks. It will also enable such services as wireless access for inventory control and convenient network access for conference rooms around LLNL. Wireless network access has the potential to increase productivity by enabling instant access to information.

2. IEEE 802.11 Basics

Sponsored by the LAN MAN Standards Committee of the IEEE Computer Society, the 1999 edition of the 802.11 standard defined the physical layer (PHY) and the medium access control layer (MAC) for WLANs. It defined PHYs for 1 and 2 Mb/s data rates in the unlicensed 2.4-GHz radio frequency (RF) band and in the infrared (IR). The 802.11 standard is a member of the family of 802 standards issued by IEEE that include 802.3 (Ethernet) and 802.5 (token ring). It was extended twice in 1999 by 802.11a, which defined the PHY for the 5-GHz band at 6 to 54 Mb/s, and 802.11b, which defined the PHY for the 2.4-GHz band at 5.5 and 11 Mb/s.

The purpose of the 802.11 standard as defined by IEEE is "to provide wireless connectivity to automatic machinery, equipment, or stations that require rapid deployment, which may be portable or hand-held, or which may be mounted on moving vehicles within a local area."

In addition to the information provided in this paper, further information on the basics of 802.11 can be found at http://www.intelligraphics.com/articles/80211_article.html.

2.1 The PHY

The 802.11 standard has specified the PHYs shown in Table 1.

Table 1. Comparison of IEEE 802.11 PHYs.

Specified in Standard	Radio Frequency (RF)	Infrared (IR)	Mechanism	Maximum Data Rate (Mb/s)
802.11	2.4 GHz ISM		DSSS	2
802.11	2.4 GHz ISM		FHSS	2
802.11		850–950 nm	Diffuse IR	2
802.11a	5 GHz ISM		OFDM	54
802.11b	2.4 GHz ISM		DSSS	11

The Frequency Hopping Spread Spectrum (FHSS) 2.4-GHz specification and the IR specification of the original 802.11 are rarely used. The limited range (approximately 15 m) of the 5-GHz Orthogonal Frequency Division Multiplexing (OFDM) PHY makes it less appealing for most uses. Most current products implement the 802.11b Direct Sequence Spread Spectrum

(DSSS) technology for data rates up to 11 Mb/s because of its price/performance advantage. Because the other PHYs are so rarely used, the remainder of this paper assumes the use of the 2.4-GHz DSSS PHY.[1]

The goal of spread spectrum technology is to increase the throughput and reliability of transmission by using more of the frequency range. DSSS operates by converting each bit of transmission into a "chip" sequence that is essentially a string of 1's and 0's that represent either the binary 1 or 0. This chip is then sent in parallel across a wide frequency range. While this approach uses more of the available frequency range, it also greatly enhances the reliability of transmission in the presence of interference. Because each bit is represented by a chip sequence, if some portion of the chip sequence is lost because of interference, it is likely that the portion of the chip that *was* received will still be enough to distinguish the original bit.

2.2 The MAC

While the 802.11 PHY is different from that of 802.3 Ethernet, the MAC specification is similar to the 802.3 Ethernet MAC specification plus the 802.2 Logical Link Control (LLC), which makes the MAC address space of 802.11 compatible with those of the other 802 protocols. While the 802.3 Ethernet MAC is essentially Carrier Sense Multiple Access/Collision Detection (CSMA/CD), the 802.11 MAC is Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). The reason for this difference is that there is no practical way to both transmit and receive *at the same time* on the wireless medium (WM) (Geier 1999, 130). As the name implies, CSMA/CA attempts to avoid collisions on the WM by placing duration information in each MAC frame, so that receiving stations can determine how long the frame will remain on the WM. If the previous MAC frame's duration is expired and a quick check of the WM shows that it is not busy, the sending station is permitted to transmit. In this way, it is a coordinated effort, unlike that of CSMA/CD, which permits a sender to transmit any time the medium is not busy.

2.3 Ad hoc vs Infrastructure Mode

There are two different modes of operation for 802.11 devices: ad hoc (Independent Basic Service Set, IBSS) or infrastructure (Extended Service Set, ESS). An ad hoc network is usually one that exists for a limited time between two or more wireless devices that *is not* connected through an access point (AP) to a wired network. For example, two laptop users wishing to share files could set up an ad hoc network using 802.11 compatible NICs and share files over the WM without need for external media (e.g., floppy disks, flash cards).

Infrastructure mode assumes the presence of one or more APs bridging the wireless media to the wired media (see Fig. 1). The AP handles station authentication and association to the wireless network. Multiple APs connected by a distribution system (DS) can extend the range of the wireless network to a much larger area than can be covered by any one AP. In typical installations, the DS is simply the existing IP network infrastructure. For security purposes, virtual LANs (VLANs) are often used to segregate wireless traffic from other traffic on the DS. Although 802.11 allows for wireless stations to dynamically switch association from one access point to another (as would be the case of a mobile PDA user walking across a campus), it does not govern how this is to be accomplished. As a result, vendor implementations are generally not

[1] For further technical information on the lesser-used PHYs, see IEEE 802.11-1999 and IEEE 802.11a-1999.

interoperable in this respect. At the time of this writing, implementing this type of functionality requires a single vendor solution.

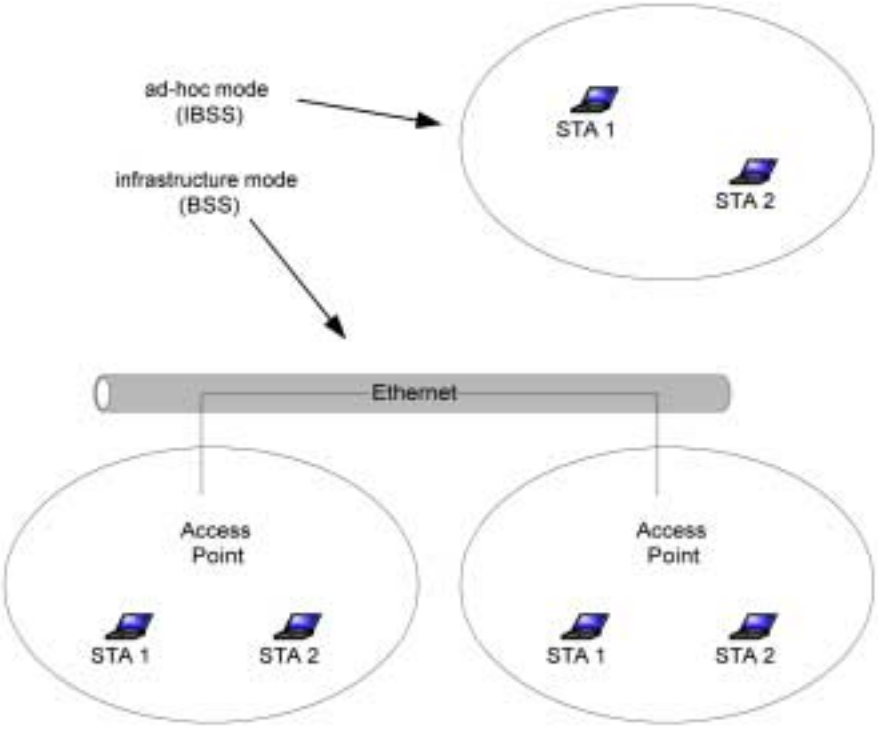

Figure 1. Ad hoc mode vs infrastructure mode.

2.4 Association and Authentication

IEEE Std. 802.11 defines an end station to AP mapping so that other stations on the wired and wireless networks have a means to contact the end station. This mapping is called "association." While end stations are permitted to dynamically associate with other APs, at any given point an end station can only be associated with one AP. An end station being "associated" with an AP is much like an Ethernet end station being placed into the bridge table of a switch. Without this mechanism, the AP would have no way of determining whether or not to forward frames received on its Ethernet port to its wireless port.

Association is a three-state process: (1) unauthenticated and unassociated; (2) authenticated and unassociated; (3) authenticated and associated.

The messages passed during these steps are called management frames. The important thing to note from this process is that association will not happen until authentication takes place. IEEE 802.11 authentication is covered in depth in Sec. 3.3.

3. Basics of WLAN Security

IEEE 802.11 contains several security features, such as open system and shared key authentication modes, the Service Set Identifier (SSID), and Wired Equivalent Privacy (WEP). Each of these features provides varying degrees of security and each is covered in this section.

Also covered is information on how RF antennas can be used to limit, and in some instances shape, the propagation of the WM.

3.1 Limiting RF Propagation

Before any other security measures are implemented, it is important to consider the implications of RF propagation by APs in a wireless network. Chosen wisely, the proper transmitter/antenna combination can be an effective security tool that will help limit access to the wireless network to only the intended coverage area. Chosen poorly, they can extend a network beyond the intended area into a parking lot or farther.

Primarily, antennas can be characterized by two features—directionality and gain. Omni-directional antennas have a 360-deg coverage area, while directional antennas limit coverage to better-defined areas (see Fig. 2). Antenna gain is typically measured in dBi[2] and is defined as the increase in power that an antenna adds to an RF signal.

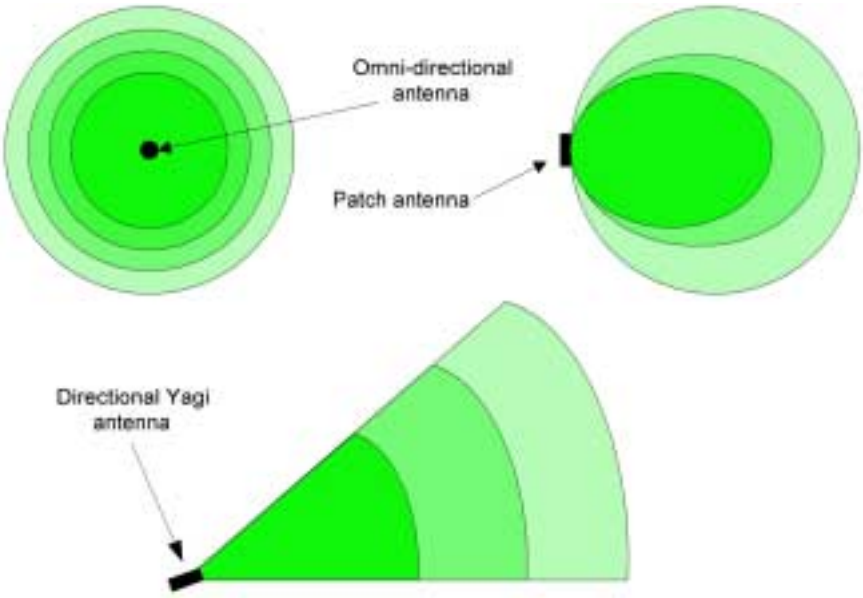

Figure 2. RF propagation patterns of common antennas.

Because current 802.11 products make use of the unlicensed Industrial, Scientific, and Medical (ISM) 2.4-GHz band, they are subject to the rules promulgated by the FCC in 1994 for spread spectrum use. These rules specify that any antenna sold with a product must be tested and approved by an FCC laboratory. To keep end users from using incorrect or illegal antennas with 802.11 products, the FCC also requires that any APs capable of using removable antennas must use nonstandard connectors.

In the U.S., the FCC defines the maximum Effective Isotropic Radiated Power (EIRP) of a transmitter/antenna combination as 36 dBm, where EIRP = transmitter power + antenna gain – cable loss. Essentially, this means that as transmitter power increases, antenna gain must decrease to remain below the 36 dBm legal maximum. For example, a 100-mW transmitter

[2] dBi is defined in reference to a theoretical isotropic (perfectly spherical propagation) antenna.

equates to 20 dBm. This transmitter combined with a 16-dBi antenna produces a total of 36 dBm, the legal limit. To increase antenna gain, we would legally be required to reduce transmitter power. In practice, most transmitter/antenna combinations sold today are well below the FCC maximum of 36 dBm.

The implications of all this are that transmitter power/antenna gain combinations are strictly regulated and limit the area that can be legally covered by any single AP. When designing WLANs, it is important to perform a thorough site survey and consider the RF propagation patterns of the antennas in use and the effective power of the transmitter/antenna combination. Also, because the ISM band is essentially open for use by anybody without licensing, it is important to consider the possibility of denial of service (DOS) from otherwise benign sources such as 2.4-GHz cordless phones. Finally, consider that a potential attacker may not be playing within the FCC rules. A resourceful attacker may be using high-power transmitters, high-gain antennas, and/or more sensitive receivers. Each of these can increase the effective range of wireless networks.

3.2 Service Set Identifier (SSID)

IEEE Std. 802.11b defines another mechanism by which to limit access: the SSID. The SSID is a network name that identifies the area covered by one or more APs. In a commonly used mode, the AP periodically broadcasts its SSID in a beacon. A wireless station wishing to associate with AP can listen for these broadcasts and can choose an AP to associate with based upon its SSID.

In another mode of operation, the SSID can be used as a security measure by configuring the AP to not broadcast its SSID. In this mode, the wireless station wishing to associate with the AP must already have its SSID configured to be the same as that of the AP. If the SSIDs are different, management frames sent to the AP from the wireless station will be rejected because they contain the incorrect SSID and association will not take place.

Unfortunately, because management frames on 802.11 WLANs are always sent in the clear, this mode of operation does not provide adequate security. An attacker can easily listen on the WM for management frames and discover the SSID of the AP. Many organizations rely upon the SSID for security without considering its limitations. This is at least partly responsible for the ease with which some WLANs are compromised.

3.3 Authentication Modes

As discussed in Sec. 2.4, before an end station can associate with an AP and gain access to the WLAN, it must perform authentication. Two types of client authentication are defined in 802.11: open system and shared key.

3.3.1 Open System Authentication

Open system authentication (Fig. 3) is a very basic form of authentication that consists of a simple authentication request containing the station ID and an authentication response containing success or failure. On success, both stations are considered to be mutually authenticated.

Figure 3. Open system authentication.

3.3.2 Shared Key Authentication

Shared key authentication (Fig. 4) is predicated on the fact that both stations taking part in the authentication process have the same "shared" key. It is assumed that this key has been transmitted to both stations through some secure channel other than the WM itself. In typical implementations, this might be set manually on the client station and the AP. The first and fourth frames of shared key authentication are similar to those found in open system authentication. The difference is that in the second and third frames, the authenticating station receives a challenge text packet (created using the WEP Pseudo Random Number Generator (PRNG)) from the AP, encrypts it using the shared key, and sends it back to the AP. If, after decryption, the challenge text matches, then one-way authentication is successful. To obtain mutual authentication, the process is repeated in the opposite direction. The fact that most attacks on 802.11b WLANs are based on capturing the encrypted form of a known response makes this form of authentication a very poor choice. It gives would-be hackers exactly the information needed to defeat WEP encryption and is why shared key authentication is never recommended. It is better to use open authentication, which will allow authentication without the correct WEP key. Limited security is still maintained because the station will not be able to send or receive data correctly with an invalid WEP key (Paulo 2001, 12).

Figure 4. Shared key authentication.

3.4 WEP

As stated by the IEEE, WEP is designed to protect users of a WLAN from casual eavesdropping and was intended to have the following properties:

- **Reasonably strong encryption**. It relies on the difficulty of recovering the secret key through a brute force attack. The difficulty grows with key length.
- **Self-synchronizing**. No need to deal with lost packets. Each packet contains the information required to decrypt it.
- **Efficient**. It can be reasonably implemented in software.

- **Exportable**. Limiting the key length leads to a greater possibility of export beyond U.S. borders.

The WEP algorithm is essentially the RC4 cryptographic algorithm from RSA Data Security, Inc. It is considered a symmetric algorithm because it uses the same key for enciphering and deciphering the plaintext Protocol Data Unit (PDU). For each transmission, the plaintext is bitwise XORed with a pseudorandom keystream to produce cyphertext. The process is reversed for decryption.

The algorithm operates as follows:

- It is assumed that the secret key has been distributed to both the transmitting and receiving stations by some secure means.
- On the transmitting station, the 40-bit secret key is concatenated with a 24-bit Initialization Vector (IV) to produce a *seed* for input into the WEP PRNG.
- The seed is passed into the PRNG to produce a stream (*keystream*) of pseudo-random octets.
- The plaintext PDU is then XORed with the pseudo-random keystream to produce the cyphertext PDU.
- This cyphertext PDU is then concatenated with the IV and transmitted on the WM.
- The receiving station reads the IV and concatenates it with the secret key, producing the seed that it passes to the PRNG.
- The receiver's PRNG should produce the identical keystream used by the transmitting station, so that when XORed with the cyphertext, the original plaintext PDU is produced.

It is worth mentioning that the plaintext PDU is also protected with a CRC to prevent random tampering with the cyphertext in transit. Unfortunately, the specification does not include any rules regarding use of the IV, except to say that the IV *may* be changed "as frequently as every MPDU." The specification does, however, encourage implementers to consider the dangers of poor IV management. This is in some part responsible for the ease with which some WEP implementations are compromised.

4. The State of WLAN Security, August 2001

The 802.11b standard has come under fire from many directions in the last few months regarding security. There have been papers published by researchers at UC Berkeley, the University of Maryland, and elsewhere that expose significant security holes in the standard. Appendix A summarizes the known problems with 802.11 WLANs and presents an objective look at the risks associated with using the technology.

The implication of the papers written to date is that WEP is completely inadequate for providing privacy on a wireless network. Among the recommendations are the following (Stubblefield, Ioannidis, and Rubin 2001):

- Assume that the link layer offers no security.
- Use higher-level mechanisms such as IPsec and SSH for security, instead of relying on WEP.

- Treat all systems that are connected via 802.11 as external. Place all access points outside the firewall.
- Assume that anyone within physical range can communicate on the network as a valid user. Keep in mind that an adversary may utilize a sophisticated antenna with much longer range than may be found on a typical 802.11 PC card.

5. WLAN Security Architecture Examples

The following WLAN architectures are meant to be a survey of possible approaches. They do not address the issue of any higher layer encryption of per-packet data on the WM, such as a Virtual Private Network (VPN). In all cases it is assumed that a VPN solution could be layered on top of any architecture for greatly increased security. The security measures discussed below are only intended to protect traffic transmitted between APs and client radios. It is therefore assumed that the existing wired network is already protected by some acceptable means.

Note also the omission of SSID from the discussion below. The SSID provides very little security because of its "clear text" nature and is therefore not of much interest when discussing security architectures. In fact, it is so security insignificant that for all of the architectures below we assume that the AP is configured to broadcast the SSID in its beacon.

The following is a partial list of known WLAN architectures and their individual pros and cons. An attempt has been made to place them in order of complexity, with the least complex solutions listed first and the last few architectures being roughly equivalent in complexity. Table 2 compares the features of WLAN security architectures.

Open Authentication without WEP (Fig. 3)

- Pros: no administrative overhead; any client can associate with the AP without any additional configuration.
- Cons: no security other than MAC address based filtering.

Open Authentication with WEP (Fig. 3)

- Pros: good enough security to deter casual intruders; fairly low administrative overhead.
- Cons: ubiquitous WEP keys are likely to be compromised.

Shared Key Authentication with WEP (Fig. 4)

- Pros: good enough security to deter casual intruders; fairly low administrative overhead.
- Cons: **uses an insecure challenge/response mechanism**; ubiquitous WEP keys are likely to be compromised.

LAWN/MOWER/Open Authentication

LAWN/MOWER is an architecture developed by Georgia Tech that makes use of common protocols and open source software to segregate users on the WLAN until they have successfully authenticated to a backend Kerberos-based account system. Once authenticated, rules are added to the router that allow the client to communicate with the internal wired network. As an added measure of security, the MAC and IP address of the client are hard-coded in the MOWER ARP cache.

- Pros: platform independent (only SSL capable browser required); based on freely available open source software; fairly strong authentication (128-bit SSL and Kerberos).
- Cons: no access outside WLAN without authentication.

NASA Ames Wireless Firewall Gateway (WFG)

The WFG is similar to that of LAWN/MOWER except that the backend account database is RADIUS-based rather than Kerberos-based. The WFG is designed around a single platform capable of routing, packet filtering, authentication, and DHCP. It operates by assigning IP addresses through DHCP, authenticating users through an SSL encrypted web page, permitting communication for the authenticated IP through the gateway, and logging. When the DHCP lease is freed, released, expired or reset, the WFG removes the firewall entries for that address. This partially addresses the concern over hijacking of an authenticated IP after a legitimate user has left the network.

- Pros: platform independent; based on open source software; central username/password administration.
- Cons: no access outside WLAN without authentication.

Cisco LEAP/RADIUS (Per Session WEP + Password Authentication) (Fig. 5)

- Pros: username/password authentication; central username/password administration; per session WEP derived from username/password.
- Cons: Cisco proprietary although it is mostly based on AAA standards (except for LEAP); fair amount of complexity; when using VPN the administrative costs are significant considering the questionable added security; client software (drivers, firmware, utilities) still has bugs and minor annoyances.

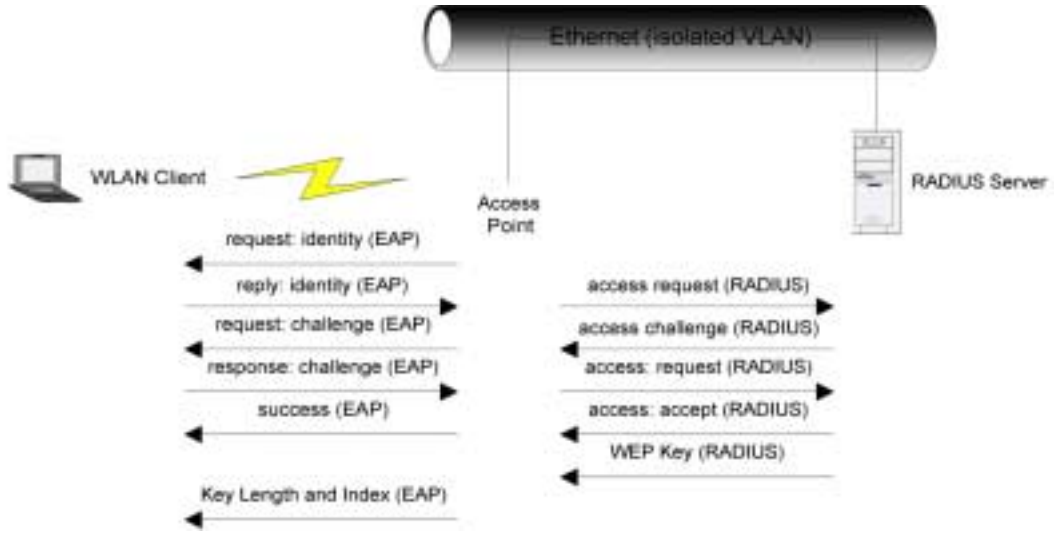

Figure 5. Cisco LEAP/RADIUS authentication.

Table 2. Features of WLAN security architectures.

Feature	Open Authentication w/WEP	LAWN/MOWER	WFG	LEAP/RADIUS
Per-packet encryption	√			√
Per-session/per-user WEP key				√
Username/password authentication		√	√	√
Logging	√	√	√	√
Platform independent	√	√	√	
Open source		√	√	
Low administrative overhead	√			
Windows integrated login				√

6. Recommended Architecture

Considering the security concerns discussed in previous sections, this paper proposes a WLAN architecture based upon the following principles:

1. The wireless network should be treated as inherently insecure. As such, it should reside outside any institutional firewalls.
2. Given that WEP encryption can be broken with commonly known algorithms, it should not be relied upon for data security.
3. WEP by itself provides at least some protection from the casual intruder and should be used if administrative costs are low.
4. If strong data encryption is required, a VPN/IPsec solution should be used.
5. Because access to the wireless network is harder to control than access to its wired counterpart, care should be taken when providing access from WLANs to other networks (even the Internet) without prior authentication.

6.1 Architecture Overview

The proposed architecture (shown in Fig. 6) has the obvious feature of placing the wireless network outside of the institutional firewall(s). In addition, it uses static WEP keys on the WLAN to keep administrative costs low and provides a Network Intrusion Detection (NID) facility to monitor possible attacks emanating from the WLAN to the Internet and other networks.

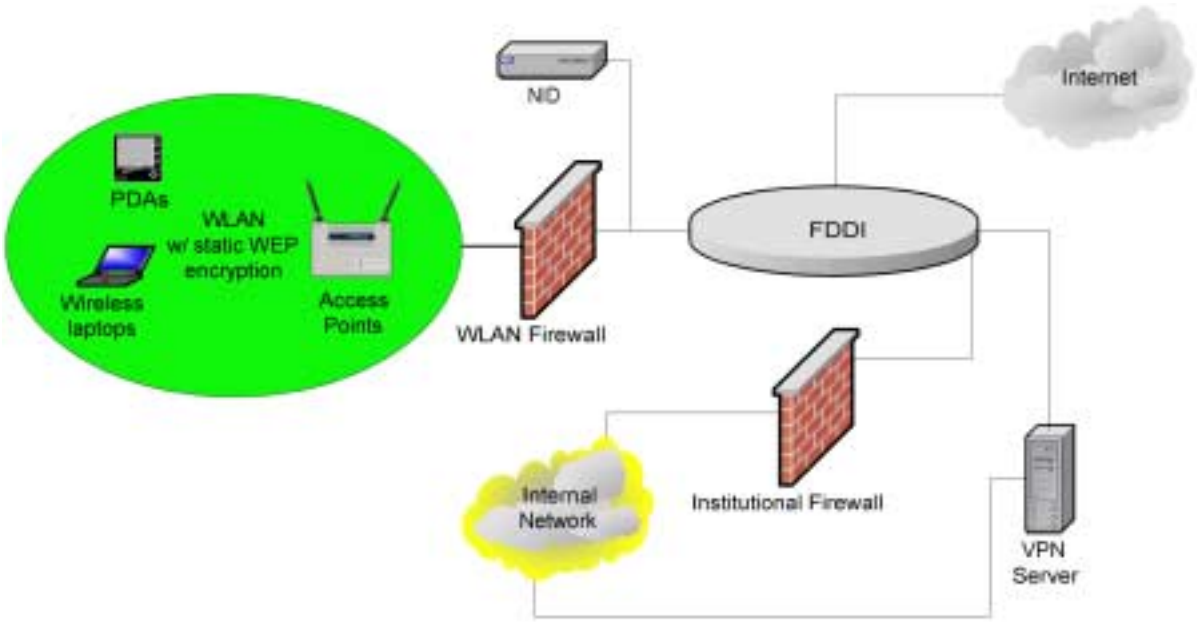

Figure 6. Proposed WLAN architecture.

As part of this architecture, it is recommended that neither the IP address range nor the domain name of the wireless network be associated with any of the existing internal networks. This will allow for better segregation of wireless traffic and will assist in identifying and filtering traffic to/from this network.

The proposed architecture incorporates most of the original design principles while allowing some degree of access to the Internet from non-VPN, non-authenticated users. The WLAN is treated as though it were an untrusted network, like the Internet. Assuming that RF propagation is limited by a thorough site survey and the use of proper antenna and transmitter power settings, the WLAN does not represent any more significant a threat to internal networks than the Internet itself.

Because roaming between APs is still in the proprietary domain, it is **highly** recommended that all APs be purchased from the same vendor. This will ensure that an end station equipped with any 802.11-compatible NIC will be able to roam between APs. In addition, any new vendor-specific security improvements that are introduced may require homogenous APs.

See Appendix B for discussion regarding the user perspective of this network.

7. Next Steps

Because LLNL already has in place much of the needed infrastructure shown in Fig. 6, integration of a wireless network can be accomplished more quickly than would otherwise be possible. It is recommended that a phased approach to implementation be taken that would first establish a small user pilot in one or two geographically strategic buildings (Phase 1), then would roll out the complete architecture to any area that requires access (Phase 2).

If the NID cannot be delivered in a reasonable time, the Phase 1 pilot could be designed without the NID in a way that would mitigate non-LLNL access to the pilot network. By using buildings

near the geographic center of the Laboratory, low-gain antennas, and low-power settings, propagation of the wireless signal could be limited to a relatively small area well within the confines of the Laboratory. Subject to these conditions, it is recommended that the Phase 1 pilot begin immediately. If not implemented at the outset, the NID will be introduced into the pilot as funding and resources become available.

The Phase 1 pilot will allow information to be gathered on the user experience and on any unforeseen security implications that will be used for planning the Phase 2 full implementation.

Appendix A—Major Papers on 802.11 Security

The following is a brief synopsis of three major papers written on 802.11 security, listed in chronological order.

Intercepting Mobile Communications: The Insecurity of 802.11
(Borisov, Goldberg, and Wagner 2001)

Otherwise known as the "Berkeley paper," this was to be the first in a series of papers that exposed in detail the weaknesses of the RC4 cryptographic algorithm and the way in which it is used in the 802.11 standard. The paper points out that the way in which RC4 is used within WEP exposes the protocol to both passive and active attacks that allow eavesdropping on, and modification to, wireless transmissions. What makes these attacks possible is the fact that the IV is normally passed in the clear at the beginning of each transmission. See Sec. 3.4 for more information on the use of the IV within WEP.

The main focus of the Berkeley paper is proving that it is possible to decrypt WEP encrypted data without having the secret key. By capturing two transmissions that use the same IV, an attacker can effectively cancel out the keystream by XORing the two cyphertexts. This, then, produces the XOR of the two original plaintexts. If one of the plaintexts is known, then the other can be derived, as can the keystream be used to generate both. A dictionary can then be created that specifies the keystream used for each IV. In this way, an attacker can eventually decrypt all transmissions on the WM without ever actually obtaining the secret key.

The authors demonstrate that IV reuse is nearly impossible to avoid, because 802.11 specifies an IV length of 24 bits. Even with 128-bit WEP, the situation does not improve, because even though the key is now (128 – 24) or 104 bits in length, the IV is still only 24 bits as specified by 802.11. In addition, many vendors restart the IV at zero each time the card is restarted and increment it by one for each subsequent transmission. This has the undesirable consequence of reusing many of the low-order IV values repeatedly.

Another attack, mentioned briefly, involves only TCP. By capturing an encrypted transmission and judiciously flipping certain bits and transmitting it back on the WM, it is possible to learn the plaintext bits of an encrypted transmission. This attack makes use of TCP's ACK mechanism to infer information about the encrypted plaintext.

Cisco wrote a response to this paper[3] pointing out that their (currently proprietary) architecture based on the Extensible Authentication Protocol (EAP) and Remote Authentication Dial-In User Service (RADIUS) alleviates some of these concerns. The Berkeley paper assumes (perhaps correctly) that because 802.11 does not define a mechanism by which to distribute the secret keys for WEP, most installations will simply use a single WEP key across the entire WLAN, if they use WEP at all. This creates a large window of opportunity for an attacker to capture IV reuse. Cisco has implemented a method to distribute per-user, per-session WEP keys along with mutual authentication based on EAP and RADIUS. In addition, Cisco starts the IV at a random value instead of at zero, as other vendors have done. Effectively shrinking the window under which a particular WEP secret key is used and increasing the time before IV reuse largely mitigates many of the concerns listed above. However, even with this architecture, WEP should

[3] http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1281_pp.htm

not be considered secure for highly sensitive communications. Cisco and others recommend using VPN technology if privacy and security are real concerns.

Your 802.11 Wireless Network Has No Clothes
(Arbaugh, Shankar, and Wan 2001)

Whereas the Berkeley paper focused in detail on WEP, this paper, known as the "Maryland paper," describes several more obvious "features" of 802.11 that expose it to attack. The authors focus on the protocols used for authentication and access control and make several points that should be fairly obvious to anyone who is familiar with the 802.11 standard and has worked with the products.

The authors correctly point out that the SSID is worthless as a security mechanism. Because it is transmitted in the clear within many of the 802.11 management frames, it is very easy to use a network "sniffer" to capture the SSID and gain access to a WLAN. They also correctly point out that both of the authentication mechanisms in the specification, open authentication and shared key authentication, are very weak. Open authentication is essentially a "null" authentication, as it was designed to be. Any request for authentication by a wireless station to the WLAN will be granted. Shared key authentication, as described in Sec. 3.2, is a basic challenge–response authentication that allows an attacker to determine the keystream used to encrypt the response and reuse this same keystream to gain authentication to the WLAN, even though the challenge text is generated by the PRNG for each authentication exchange.

The authors also comment on the insecurity of proprietary Access Control Lists (ACLs) found on many products today. Most ACLs are used to limit access to a list of known MAC addresses. However, because most 802.11 adapters allow their MAC address to be modified in software, this is a very poor form of security. It is a relatively simple procedure to sniff the WLAN for MAC addresses that are permitted access, change the MAC address of the 802.11 adapter, and gain access to the WLAN.

Finally, the authors provide some recommendations to mitigate some of these security concerns. They highlight a better WEP key management system and use of higher layer security mechanisms, such as IPsec or VPN.

Cisco also responded to this paper,[4] acknowledging and agreeing with most of the authors' comments except those about the manual changing of WEP keys. The 802.11 standard does not define any mechanisms for distribution of WEP keys; therefore, most keys are entered manually. However, Cisco's solution does provide for the distribution of per-user, per-session keys.

Weaknesses in the Key Scheduling Algorithm of RC4
(Fluhrer, Mantin, and Shamir 2001)

To date, this paper is the most significant and in-depth discussion of weaknesses within RC4, the underlying encryption mechanism used by WEP. The authors introduce a new attack on WEP that is a passive, cyphertext-only attack able to retrieve the entire secret key (not just the keystream generated by a particular IV, but the actual key) in a relatively small amount of time, about 4,000,000 packets. In addition, the attack grows linearly regardless of key or IV size.

[4] http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1327_pp.htm

The attack makes use of a flaw in the WEP protocol that allows an attacker to glean information about key bytes given knowledge of the IV and the first output byte. As demonstrated by researchers at AT&T, the first byte in most, if not all, WEP encrypted transmissions is the 802.2 LLC header that contains 0xAA, or the SNAP designation (Stubblefield, Ioannidis, and Rubin 2001). Then, because the IV is transmitted in the clear as specified by 802.11, attackers have the two requirements to execute this attack.

Although the authors of this paper mention that they "have not attempted to attack an actual WEP connection, and hence do not claim that WEP is actually vulnerable to this attack," the researchers at AT&T *did* implement the attack against WEP using a $100 802.11 NIC in a Linux host with slight modifications to freely available source code. They were able to recover the entire secret key in about 5,000,000 packets, which represented about 3 hours on a partially loaded network (Stubblefield, Ioannidis, and Rubin 2001).

Appendix B—User Perspective

To use this network, it is assumed that end stations are equipped with 802.11-compatible NICs and that those NICs support, and are configured for, WEP. The APs will be configured in such a way that they will not allow an end station to associate without the use of WEP. This will keep people from unknowingly sending data in the clear.

This implies that visitors to LLNL and Laboratory employees will need to have either knowledge of the WEP key or to have it entered by a system administrator prior to accessing the wireless network. Policy and procedures surrounding the management of the WEP key are not covered in this paper, but it should be noted that a well-protected WEP key will yield a better-protected wireless network.

Once connected to the network via WEP, access to the Internet will be available without authentication. Any further access into internal networks will require use of the Laboratory VPN service.

It may be necessary for users of the LLNL wireless network to turn off WEP encryption when making use of public wireless networks such as those offered at many conferences and trade shows. At this time, it appears that end users will not need “administrator” privileges under Microsoft Windows operating systems to enable/disable WEP encryption or to modify WEP keys. They will, however, require a separate password for the tool used to change WEP keys.

It is anticipated that working with WEP encryption will require some level of knowledge to change the various settings related to WEP. The creation of a standard set of guidelines is highly recommended.

Because RF carries the risk of piggybacking classified information on otherwise innocuous transmissions, users should be required to remove wireless NICs when entering “limited” areas. The policy should be similar in intent to those concerning cellular telephones, and infractions of the wireless NIC policy should entail a similar response.

References

Arbaugh, W. A., N. Shankar, and Y. C. J. Wan (March 30, 2001), *Your 802.11 Wireless Network Has No Clothes*, Department of Computer Science, University of Maryland, College Park.

Borisov, N., I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," in *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking* (Association for Computing Machinery, New York, NY), p. 180.

Fluhrer, S., I. Mantin, and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," presented at the *Eighth Annual Workshop on Selected Areas in Cryptography*, August 16–17, 2001, Toronto, Canada.

Geier, J. (1999), *Wireless LANS: Implementing Interoperable Networks* (Macmillan Technical Publishing, Indianapolis, IN).

LAN MAN Standards Committee of the IEEE Computer Society, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ANSI/IEEE Std 802.11, 1999.

LAN MAN Standards Committee of the IEEE Computer Society*, High-Speed Physical Layer in the 5GHz Band*, ANSI/IEEE Std 802.11a, 1999.

LAN MAN Standards Committee of the IEEE Computer Society, *High-Speed Physical Layer Extension in the 2.4 GHz Band*, ANSI/IEEE Std 802.11b, 1999.

Paulo, G. (June 2001), *Free & Easy Wireless Networking?: A Wi-Fi Security Update* (Cahners In-Stat Group, Cahners Business Information), LN0103WL.

Stubblefield, A., J. Ioannidis, and A. D. Rubin (August 21, 2001), *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*, AT&T Labs Technical Report TD-4ZCPZZ, Rev. 2.